**Занятие 5. ПОСТРОЕНИЕ СЕТЕЙ IP-ТЕЛЕФОНИИ**

**НА БАЗЕ ПРОТОКОЛА SIP**

**5.1. Функциональные возможности протокола**

Вторым вариантом построения сетей стал протокол SIP, разработанный группой MMUSIC (Multiparty Multime-dia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543

Протокол инициирования сеансов - Session Initiation Protocol (SIP)- является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации, в основу которого заложены следующие принципы.

*Персональная мобильность пользователей.* Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится.

Для этого пользователь с помощью специального сообщения - REGISTER - информирует о своих перемещениях сервер определения местоположения.

*Масштабируемость сети* характеризуется,в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.

*Расширяемость протокола* характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

*Интеграция в стек существующих протоколов Интернет*. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом Internet Engineering Task Force (IETF).

*Взаимодействие с другими протоколами сигнализации.*Протокол SIP может быть использован совместно с протоколом Н.323. Возможно также взаимодействие протокола SIP с системами сигнализации ТфОП - DSS1 и ОКС7.

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. В качестве транспорта могут использоваться протоколы Х.25, Frame Relay, AAL5, IPX и др. Структура сообщений SIP не зависит от выбранной транспортной технологии. Но в то же время предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP.

Здесь же следует отметить, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом ТСР (рис. 5.1) По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходимо известить встречную сторону, какого рода информация может приниматься (передаваться), алгоритм ее кодирования и адрес, на который ее следует передавать. Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между предполагаемыми участниками этой связи данными об их функциональных возможностях. Для этой цели чаще всего используется протокол описания сеансов связи SDP (Session Description Protocol). В течение сеанса связи может производиться его модификация, поэтому предусмотрена передача средствами SDP сообщений SIP с новыми описаниями сеанса.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP, но сам протокол SIP не исключает возможность применения для этих целей других протоколов.

**5.2. Адресация**

Для того чтобы вызвать кого-то, необходимо знать его адрес или хотя бы имя. В сети Интернет для нахождения хоста используется URL (для SIP он обозначается как SIP URL). В качестве адреса в SIP выбран самый распространенный тип - адрес электронной почты. Он уже сейчас является основным адресом, не зависящим от местоположения пользователя. Существуют четыре основные формы адреса: **имя@домен, имя@хост, имя@IP-адрес, №телефона-@шлюз.**

Адрес состоит из двух частей. Первая - это та часть, в которой указывается адрес домена, хоста или шлюза. Она может быть представлена и alias-адресом; тогда, чтобы найти IP-адрес, необходимо обратиться к сервису системы DNS. Если же здесь помещен IP-адрес, то никакого преобразования не надо, так как в этом случае достаточно напрямую связаться с адресатом.

Вторая часть адреса - это имя пользователя в домене или хосте. Если в первой части указан адрес шлюза, то вторая часть представлена телефонным номером абонента в глобальной или частной системе нумерации.

В начале адреса ставятся слово sip, указывающее, что это именно SIP-адрес, так как бывают другие (например, mailto).

SIP-адрес может соответствовать разным физическим адресам в зависимости от времени суток, алгоритма работы и т.п. Он может направлять вызов к одному определенному пользователю, первому свободному из группы пользователей или ко всей группе. Благодаря этому можно организовать такие услуги, как ночной вызов, переадресация, конференция и др.

Возможно использование адреса электронной почты в качестве публикуемого SIP-адреса. Применение URL позволяет, например, размещать свой адрес на Web-страницах:

sip: user1@rts.loniis.ru

sip: user1@ 195.201.37.104

sip: 273-44-55@gateway.ru

**5.3. Элементы SIP-сети**

Сеть SIP содержит следующие основные элементы.

*Агент пользователя* (User Agent или SIP client) является приложением терминального оборудования и включает в себя две составляющие: клиент агента пользователя (User Agent Client - UAC) и сервер агента пользователя (User Agent Server - UAS), иначе называемые *клиент*и*сервер*. Клиент UAC инициирует SIP-запросы, т.е. выступает в качестве вызывающей стороны. Сервер UAS принимает запросы и отвечает на них, т.е. выступает в качестве вызываемой стороны.

Запросы могут передаваться не прямо адресату, а на некоторый промежуточный узел. Такие узлы бывают двух основных типов: прокси-сервер и сервер переадресации

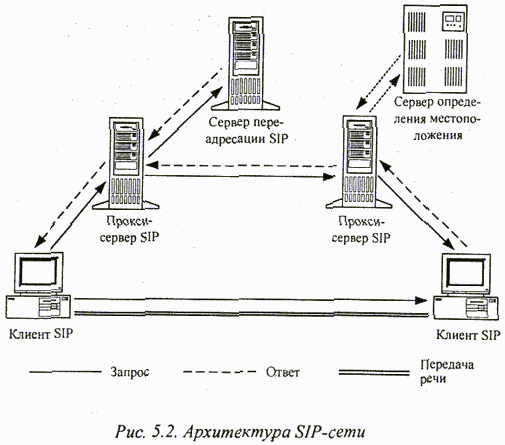
*Прокси-сервер* (proxy server**)**принимает запросы, обрабатывает их и отправляет дальше на следующий сервер, который может быть как другим прокси-сервером, так и последним UAS. Таким образом, прокси-сервер принимает и отправляет запросы и клиента, и сервера. Приняв запрос

от UAC, прокси-сервер действует от имени этого UAC.

Существует два вида прокси-серверов: с сохранением состояний (stateful) и без сохранения состояний (stateless). Сервер первого типа хранит в памяти входящий запрос, который явился причиной генерации одного или нескольких исходящих запросов. Эти исходящие запросы сервер также запоминает. Все запросы хранятся в памяти сервера только до окончания транзакции, т.е. до получения ответов на за просы. Сервер без сохранения состояний просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер 1-го типа, так как ресурс процессора не тратится на запоминание состояний, вследствие чего сервер этого типа может обслужить большее количество пользователей.

|  |  |
| --- | --- |
| Протокол инициирования сеансов связи ( SIP ) | Прикладной уровень |
| Протоколы TCP и UDP | Транспортный уровень |
| Протоколы IPv4 и IPv6 | Сетевой уровень |
| PPP, AAL5.     ATM, Ethernet, V.34. | Уровень звена данных |
| UTP5, ВОЛС и др. | Физический уровень |

Рис. 5.1. Место протокола SIP в стеке протоколов TCP/IP



Прокси-сервер может модифицировать запросы, которые он переправляет дальше. Проще говоря, пользователь отсылает требование установить соединение на прокси-сер-вер, а тот сам “заботится” о том, чтобы оно было установлено. Прокси-сервер может размножать запрос и передавать его по разным направлениям, чтобы запрос достиг нескольких мест, в надежде на то, что нужный пользователь окажется в одном из них.

*Сервер переадресации***(**redirect server**)**передает клиенту в ответе на запрос адрес следующего сервера или клиента, с которым первый клиент связывается затем непосредственно. Он не может инициировать собственные запросы. Адрес сообщается первому клиенту в поле Contact сообщений SIP. Таким образом, этот сервер просто выполняет функции поиска текущего адреса пользователя.

Пользователь может перемещаться от одной оконечной системы к другой, так что нужен какой-то метод определения его местоположения (рис. 5.2). Для этого в SIP используется *сервер местоположения* (location server) - это база адресов, доступ к которой имеют SIP-серверы, пользующиеся ее услугами для получения информации о возможном местоположении вызываемого пользователя. Принципы работы сервера местоположения не регламентированы документом RFC 2543, но там имеются примеры протоколов, которые могут использоваться для этого LDAP (RFC 1777), rwnois (RFC 2167) и др. Упрощенно базу данных можно представить как совокупность адресных записей, в которых напротив “публикуемого” адреса пользователя его стоит текущий адрес. Приняв запрос, сервер SIP обращается к серверу местоположения, чтобы узнать адрес, по которому можно найти пользователя. В ответ тот сообщает либо список возможных адресов, либо информирует о невозможности найти их. С другой стороны, пользователь информирует SIP-сервер о своем местоположении сообщением REGISTER. Сервер местоположения может располагаться как совместно с SIP-сервером (рис. 5.2), где могут присутствовать некоторые элементы базы адресов, так и отдельно от него.

**Контрольные вопросы**

1. Зачем нужен протокол SIP?

2. Основные принципы, положенные в основу протокола SIP, кто его стандартизировал?

3. Какое место занимает протокол SIP в стеке протоколов TCP/IP.

4. С помощью какого протокола терминалы обмениваются информацией о своих функциональных возможностях?

5. Перечислить основные элементы SIP-сети.

6. Какой тип адресации используется в протоколе SIP.

7. Перечислить типы SIP-адресов,что значат их элементы?

**Контрольное задание**

1. Элементы SIP-сети, их функции.

2. Агент пользователя и его элементы.

3. Прокси-сервер: типы и функции.

4. Сервер переадресации, его функции.

5. Сервер определения местоположения, его функции.

6. Описать процесс установления соединения между терминалами на примере SIP-сети

## Занятие 6. Сообщения SIP

### 6.1. Структура сообщений

Согласно архитектуре “клиент-сервер” все сообщения делятся на запросы, передаваемые от клиента к серверу, и на ответы сервера клиенту.

Например, чтобы инициировать установление соединения, вызывающий пользователь должен сообщить серверу ряд параметров, в частности, адрес вызываемого пользователя, параметры информационных каналов и др. Эти параметры передаются в специальном SIP-запросе. От вызываемого пользователя к вызывающему передается ответ на запрос, также содержащий ряд параметров.

Все сообщения протокола SIP (запросы и ответы), представляют собой последовательности текстовых строк, закодированных в соответствии с документом RFC 2279. Структура и синтаксис сообщений SIP (рис. 6.1) соответствуют используемым в протоколе НТТР.

Стартовая строка представляет собой начальную строку любого SIP-сообщения. Если сообщение является запросом, в этой строке указываются тип запроса, адресат и номер версии протокола. Если сообщение является ответом на запрос, в стартовой строке указываются номер версии протокола, тип ответа и его короткая расшифровка, предназначенная только для обслуживающего персонала и необрабатываемая клиентом.

Заголовки сообщений содержат сведения об отправителе, адресате, пути следования и др., в общем, переносят информацию, необходимую для обслуживания данного сообщения. О типе заголовка можно узнать по его имени. Оно не зависит от регистра (т.е. буквы могут быть прописные и строчные), но обычно имя пишут с большой буквы, за которой идут строчные.

Сообщения протокола SIP могут содержать так называемое тело сообщения. В сообщениях ACK, INVITE и OPTIONS тело сообщения содержит описание сеансов связи, например, в формате протокола SDP. Сообщение BYE тела сообщения не содержит, а ситуация с сообщением REGISTER подлежит дальнейшему изучению. С ответами дело обстоит иначе: любой ответ может содержать тело сообщения, но содержимое тела в ответах разных типов бывает разным. Вся информация, необходимая для установления соединения, помещается в заголовке. Это может быть, например, адрес вызываемого и вызывающего пользователей, пройденный сообщением путь или размер тела сообщения. О заголовке и содержащейся в нем информации можно узнать по имени, которое всегда начинается с прописной буквы, далее следуют строчные. Некоторые заголовки используются во всех сообщениях, а некоторые - только в определенных случаях.

Существуют заголовки четырех видов:

* общие (и в запросах, и ответах);
* содержания (начинаются со слова **Content** и несут информацию о размере тела сообщения или об источнике, передавшем сообщение);
* запросов (дополнительная информация о запросе);
* ответов (дополнительная информация об ответе).

Заголовок содержит имя, за которым после двоеточия (**:**) следует поле, содержащее данные заголовка,

т.е. **имя:со-держимое***.*

Примеры наиболее часто встречающихся заголовков.

**Call-ID -**уникальный идентификатор отдельного сеанса связи или регистрации отдельного клиента; он подобен метке соединения (call reference) в DSS-1. Назначается стороной, которая инициирует вызов. Содержит буквенно-числовое значение и имя хоста, разделенное символом **@:**

**2345call@rts.loniis.ru**

**To -**определяет получателя запроса; кроме SIP-адреса, здесь может присутствовать параметр **tag** для идентификации пользователя или услуги, находящихся в одном SIP URL. Если необходим визуальный вывод имени пользователя, например, на дисплей, его также можно поместить в поле **То**:

**the director <userA@loniis.ru> tag=12345.**

**From -**определяет отправителя запроса (по организации аналогичен полю **То**).

**CSeq**- уникальный идентификатор запроса внутри одного **Call-ID**; необходим, чтобы отличить, на какой запрос прошел ответ, так как иногда он может оказаться ответом на другой запрос; состоит из двух частей: натурального числа (от 1 до 232) и типа запроса.

Заголовок **Via**служит, для того чтобы избежать ситуации, в которых запрос пойдет по замкнутому пути, а также для тех случаев, когда необходимо, чтобы запросы и ответы обязательно проходили по одному и тому же пути (например, в случае использования межсетевого экрана - firewall). Запрос может проходить через несколько прокси-серверов, каждый из которых принимает, обрабатывает и переправляет его к следующему прокси-серверу и так до тех пор, пока запрос не попадет к адресату. Таким образом, в заголовке **Via** указывается весь путь, пройденный запросом: каждый прокси-сервер добавляет в запрос поле со своим адресом. Например, запрос на своем пути обрабатывался двумя прокси-серверами: сначала сервером loniis.ru, потом sip.tele-com.com. Тогда в запросе появятся следующие поля:

**Via: SIP/2.0/UDP sip.telecom.com:5060**

**Via: SIP/2.0/UDP loniis.ru:5060**

**Content-Type -**определяет формат описания сеанса связи. Само описание сеанса, например, в формате протокола SDP, включается в тело сообщения.

**Content**-**Length -**показывает размер тела сообщения.

### 6.2. Запросы

В настоящей версии протокола SIP определено 6 типов запросов. Каждый из них предназначен для выполнения довольно широкого круга задач, что является явным достоинством протокола SIP, так как благодаря этому число сообщений, которыми обмениваются терминалы и серверы, сведено к минимуму. С помощью запросов клиент сообщает

о текущем местоположении, приглашает пользователей

|  |
| --- |
| Стартовая строка |
| Заголовки |
| Пустая строка |
| Тело сообщения |

*Рис. 6.1. Структура сообщений протокола SIP*

INVITE sip: [watson@boston.bell](mailto:watson@boston.bell)-tel.com SIP/2.0

Via: SIP/2.0/UDP kton.bell-tel.com

From: A.Bell <sip: a.g.bell@bell-tel.com>

To: T.Watson <sip: watson@bell-tel.com>

Сall-ID: [3298420296@kton.bell](mailto:3298420296@kton.bell)-tel.com

Cseq: 1 INVITE

Content-Type: application/sdp

Content-Length: ...

v =0

0 =bell 53655765  2353687637  IN IP4 128.3.4.5

SIP =IN IP4 kton.bell-tel.com

m =audio 3456 RTP/ AVP 0 3 4 5

*Рис. 6.2. Пример SIP-запросов*

принять участие всеансах связи, модифицирует уже установленные сеансы, завершает их и т.д. Сервер определяет тип принятого запроса по названию, указанному в стартовой строке. В той же строке в поле **Request-URI** указан SIP-адрес вызываемого пользователя. Описание запросов приведено ниже.

INVITE - приглашает пользователя принять участие в сеансе связи. Он обычно содержит описание сеанса связи, где указывается вид принимаемой информации и параметры (список возможных вариантов параметров), необходимые для приема информации, и может указываться вид информации, который вызываемый пользователь желает передавать.

В ответе на запрос INVITE указывается вид информации, которая будет приниматься или передаваться

(рис. 6.2). Этот запрос приглашает watson@bell-tel.com для участия в сеансе связи с a.g.bell@bell-tel.com. В теле сообщения отправитель указывает, что он может принимать на порт 3456 аудиоинформацию, кодированную 0 (PCMU), 3 (GSM), 4 (G.723) и 5 (DV14). Запрос направляется на прокси-сервер boston.bell-tel.com. В полях **То** и **From** перед ско-бками с адресом **< >**помещена надпись, которую пользователь желает вывести на дисплей вызываемого пользователя.

ACK - подтверждает прием от вызываемой стороны ответа на команду INVITE и завершает транзакцию.

OPTIONS - позволяет получить информацию о функциональных возможностях пользовательских агентов и сетевых серверов, но этот запрос не используется для организации сеансов связи.

BYE - используется вызывавшей и вызванной сторонами для разрушения соединения. Перед тем как разрушить соединение, пользовательские агенты отправляют этот запрос к серверу, сообщая о намерении прекратить сеанс связи.

CANCEL - позволяет пользовательским агентам и сетевым серверам отменить любой ранее переданный запрос, если финальный ответ на него (т.е. ответ с номерами 2хх, 3хх, 4хх, 5хх, 6хх) еще не получен.

REGISTER - применяется клиентами для регистрации данных о местоположении с использованием серверов SIP.

### 6.3. Ответы

После приема и интерпретации запроса, адресат (прокси-сервер) передает ответ на этот запрос. Содержание ответов: подтверждение установления соединения, передача запрошенной информации, сведения о неисправностях и т.д.

Структуры ответов и их типы протокол SIP унаследовал от протокола НТТР. Определено 6 типов ответов, несущих разную функциональную нагрузку. Тип ответа кодируется 3-значным числом. Самой важной является первая цифра, которая определяет класс ответа, остальные две цифры лишь дополняют первую. В некоторых случаях оборудование может не знать все коды ответов, но оно обязательно должно знать, как интерпретировать первую цифру. Все ответы делятся на 2 группы: информационные и финальные.

*Информационные*ответы показывают, что запрос находится в стадии обработки.

*Финальные*ответы кодируются 3-значными числами, начинающимися с цифр 2, 3, 4, 5 и 6, что означает заверше- ние обработки запроса, и содержат, когда это нужно, результаты обработки запроса (рис. 6.3):

**1хх** (информационный) - запрос принят, продолжается его обработка;

**2хх** (успех) - запрос принят, понят и успешно обработан;

**3хх** (переадресация) - для завершения обработки запроса нужны дальнейшие действия;

**4хх** (ошибка клиента) - запрос содержит ошибку и не может быть выполнен;

 SIP/2.0 200 OK

Via: SIP/2.0/UDP kton.bell-tel.com

From: A. Bell <sip:a.g.bell@bell-tel.com>

To: <sip:wstson@bell-tel.com>;

Сall-ID:3298420296@kton.bell-tel.com

Сseq: 1 INVITE

Content-Type: application/sdp

Content-Length: ...

v =0

0 =watson 4858949  4858949 IN IP4 192.1.2.3

t =3149329600 0

SIP =IN IP4 boston.bell-tel.com

m =audio 5004 RTP/AVP 0 3

a =rtpmap:0 PCMU/8000

a =rtpmap: 3 GSM/8000

*Рис. 6.3. Пример SIP-ответов*

**5хх** (ошибка сервера) - сервер не может выполнить явно правильный запрос;

**6хх** (глобальный сбой) - запрос не может быть обработан никаким сервером.

В ответе пользователя Watson на запрос Bell сообщается, что он может принимать аудиоинформацию на порт 5004, понимать кодеки PCMU, GSM. Поля **From, To, Via, Call-ID** взяты из запроса. Поле **Cseq** показывает, что - это ответ на INVITE с Cseq: 1.

**Контрольные вопросы**

1. Описать принцип “клиент-сервер”.
2. Сообщения протокола SIP, их формат и структура.
3. Существующие виды сообщений.
4. Назначение запросов и ответов протокола SIP.
5. Пояснить назначение основных заголовков сообщений.

**Контрольное задание**

Для каждого варианта составить запрос и ответ применительно к сеансу связи между вызывающим и вызываемым пользователями (табл. 6.1). Заголовки, которые нельзя составить по табл. 6.1, и тело сообщения взять из рис. 6.2 и 6.3